US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/10/2025

OPDIV:

ACF

Name:

GovDelivery

PIA Unique Identifier:

P-7397682-297845

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The purpose of the Administration on Children and Families (ACF) GovDelivery system is to help citizens and employees to get faster access to relevant services and resources from ACF by allowing them to subscribe to specific content areas on the ACF websites. Subscription topics may range from general information about ACF, to specific information based on our mission to foster health and well-being by providing federal leadership, partnership, and resources for the compassionate and effective delivery of human services.¿ Examples include news digests, funding opportunity announcements, best practices, new publications, and resources, and (for internal staff) agency communications.

Describe the type of information the system will collect, maintain (store), or share.

The GovDelivery system collects and maintains Personally Identifiable Information (PII) from public users, ACF employees, and system administrators. For public users, the system collects names, email addresses, phone numbers, passwords, and profile information to enable subscription-based communication and deliver targeted notifications. For system administrators and developers, it

stores email addresses and passwords, which may include PII if the email contains the individual's name. For ACF employees, only email addresses are collected.The PII is used to facilitate communication, manage subscriptions, and provide access controls. It enables public users to receive relevant content updates and allows administrators and developers to manage the system effectively. All PII is encrypted in transit and at rest using FIPS-compliant standards, ensuring the confidentiality and security of the data.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The ACF GovDelivery system is a subscription-based communication platform designed to enhance public engagement and streamline the dissemination of information from the Administration for Children and Families (ACF). The system enables public users and ACF employees to subscribe to specific content areas on ACF websites, receiving targeted notifications and updates.

When public users create a subscription account, the system collects and maintains the following Personally Identifiable Information (PII):

Name
Email address
Phone number (if provided)
Password (optional for securing subscriber preferences).

ACF employees and direct contractors serving as system administrators may have their email addresses stored for account provisioning and system management purposes.

All information is stored temporarily for a period of three years in accordance with the General Records Schedule (GRS), which requires data retention for three years but allows for longer retention if required for business purposes. During this period, data is encrypted in transit and at rest using FIPS-compliant and adequate encryption standards. Information is backed up until the contract expires and then retained for the legally mandated retention period. Public users can delete their accounts and associated PII from the system at any time.

For ACF employees and direct contractors subscribed via synchronization with an ACF group distribution list, only their email addresses are stored, and no individual accounts are created. After the 3-year retention period or contract expiration, all PII is permanently deleted following Granicus' data sanitization procedures to prevent unauthorized access or recovery.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
E-Mail Address
Phone Numbers
Password (optional for securing subscriber preferences)

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The primary purpose of collecting PII from the public is to provide contact information to send information.

The purpose of collecting PII from ACF employees and c ontractors is for account provisioning to administer the system.

Describe the secondary uses for which the PII will be used.

N/A

Identify legal authorities governing information use and disclosure specific to the system and program.

The legal authority governing the use and disclosure of information specific to the system and program is derived from 5 U.S.C. § 301, commonly known as the Departmental Regulations.

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Email
Online
Government Sources
Within OpDiv
Other HHS OpDiv
Non-Government Sources
Public
Commercial Data Broker

Identify the OMB information collection approval number and expiration date

Collection of Email Address and Phone Number is excluded from the Paperwork Reduction Act since the use of the information falls under the “Uses of the “general solicitations” regulatory exclusion for social media and other web-based technologies” exclusion.

Profile Form for Child Welfare Subscriptions: OMB Control Number: 0970-0531, Expiration Date: 09/30/2025

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Public users of ACF GovDelivery subscriptions are notified on the system’s website that an email address is required to subscribe.

ACF employees and direct contractors serving in system administrator and developer roles are made aware that their user information must be provided to provision account access and perform required duties.

ACF employees and direct contractors who are subscribed via a synchronization between an ACF email distribution list and GovDelivery are not given prior notice since the only information collected is a government email address and the communications sent via GovDelivery are for government business.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

For the public, a subscriber account is optional. In most circumstances, the content sent to subscribers is also available on an ACF website.

For ACF employees and direct contractors serving in system administrator and developer roles, there is no option to opt out.

For ACF employees and direct contractors who are subscribed via a synchronization between an ACF email distribution list and GovDelivery, there is no option to opt out.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

The GovDelivery system provides clear notification and consent mechanisms for individuals whose PII is collected.

For public users, notification is provided through the subscription process. When individuals subscribe to ACF communications, they are informed of the information being collected and how it will be used. If major changes occur to the system that impact PII, users will be notified via email with details on the changes, provided with the option to review and update their subscription preferences or unsubscribe altogether.

For ACF employees and direct contractors serving in the system as administrator, notification of major changes is provided through internal communication channels, including agency-wide announcements, email notifications and updated privacy policies and procedures.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

An individual may contact Granicus (vendor of GovDelivery) at support@granicus.com to “exercise any rights, in relation to personal data.” In addition, an individual can escalate an issue to the Granicus Data Protection Officer. Source: Granicus Privacy Statement.

ACF employees and direct contractors will report PII concerns through ACF Incident Response (IRT) team or the ACF Help Desk. Issues are reviewed with corrective actions applied as needed. ACF IRT will follow ACF’s breach procedures, including notification to HHS Computer Security Incident Response Center (CSIRC).

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

The following process is in place to ensure the data collected maintains its integrity, availability, accuracy, and relevancy.

Data Integrity:

The GovDelivery system employs encryption protocols and access controls to protect the integrity of the data collected. All PII is encrypted in transit and at rest using FIPS-compliant and encryption standards. Audit logs and automated monitoring mechanisms are in place to detect unauthorized modifications or data tampering, ensuring the integrity of stored information.

Data Availability:

To ensure availability, Granicus data centers host the GovDelivery system, offering redundant storage and backup processes. Data is routinely backed up and stored in compliance with federal records management policies. System uptime is maintained through continuous monitoring and failover mechanisms, ensuring uninterrupted access to the platform and the data.

Data Accuracy:
The system automatically synchronizes with user-provided data to maintain accuracy. Public users have the ability to update their subscription preferences or delete their accounts, ensuring that stored PII reflects the most current information. ACF administrators periodically review system data to verify accuracy and remove any obsolete or invalid entries.

Data Relevancy:
The GovDelivery system only collects necessary and relevant PII (example: name, email address, and phone number) required for subscription and communication purposes. The system allows users to modify or delete their accounts if the information becomes outdated. Data retention practices follow legally mandated retention periods, after which irrelevant or outdated data is securely deleted.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

ACF employees and direct contractors serving as administrators and developers can access PII as part of their duties. Access is role based and defined and approved by the system owner. The system owner assigns privileges based on assigned roles and need to know. Access is revoked upon completion of an assigned role.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

The System Owner reviews roles and grants ACF employees and direct contractors access permissions based on a right to know and a right to access PII. Development and administrative roles that do not require direct access to PII within the system are provided limited access based upon their user credentials.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All ACF employees and contractors that support the GovDelivery system must complete and comply with the annual HHS Cybersecurity Awareness Training (CSAT). This training enhances their knowledge of proper handling of Personally Identifiable Information (PII), ensuring they understand data protection requirements and best practices. By completing CSAT, employees and contractors reinforce their awareness of cybersecurity threats, phishing attempts.

Describe training system users receive (above and beyond general security and privacy awareness training).

N/A

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Below is the General Records Schedule (GRS) for the GovDelivery.

GRS 6.1, Item 12 - Support and/or administrative position

Disposition Instruction: Temporary. Delete when 3 years old, but longer retention is authorized if required for business use.

Disposition Authority: DAA-GRS-2022-0006-0003

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls

Administrative controls for GovDelivery include role-based access controls (RBAC) to ensure that users only access data necessary for their job functions. Access permissions are assigned based on the principle of least privilege and are reviewed periodically to prevent unauthorized access. The system owner is responsible for defining and approving user access levels, ensuring compliance with organizational policies. Additionally, regular training and audits are conducted to reinforce security best practices and detect potential access violations.

Technical Controls

Technical controls for GovDelivery include two-factor authentication (2FA) for ACF employees and direct contractors to enhance identity verification. Users must authenticate using a Personal Identity Verification (PIV) card and a secure user PIN before accessing the system. The system employs encryption protocols to safeguard data in transit and at rest, ensuring confidentiality and integrity. Regular security updates and vulnerability assessments are conducted to maintain system resilience against cyber threats.

Physical Controls

Physical controls for GovDelivery include restricted access to the facility through identification badges that verify personnel credentials. Closed-circuit television (CCTV) cameras are strategically placed to monitor and record activities in areas where the system is housed, deterring unauthorized entry. The facility is also equipped with alarm systems and security personnel to prevent and respond to physical security incidents. Environmental safeguards, such as fire suppression systems and climate control, are in place to protect system hardware from damage.

Identify the publicly-available URL:

https://public.govdelivery.com/accounts/USACFCWIG/subscriber/new and https://public.govdelivery.com/accounts/USACFOTIP/signup/43241

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

No

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null